I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Introductory Essay for 2008 Privacy Year in Review

PETER P. SWIRE* & MARTHA K. LANDESBERG**

I. INTRODUCTION

This essay introduces our fourth issue of Privacy Law Year in Review. With two scholarly articles and thirteen notes by law students, this issue is the most comprehensive source for current developments in privacy law, focused on the United States. We hope this issue can be a valuable desktop resource for people who work on the challenging array of information privacy topics.

The area of online advertising has drawn particular attention recently, both in the United States and the European Union. The Federal Trade Commission ("FTC") has continued to highlight issues of behavioral profiling in online advertising,[1] while the European Union has emphasized its concerns about privacy and search engines. Major online advertisers have merged, increasing the size of their

* Peter P. Swire is the C. William O'Neill Professor of Law and Judicial Administration, Moritz College of Law at The Ohio State University, and Senior Fellow, Center for American Progress. From 1999 until early 2001, Professor Swire served as Chief Counselor for Privacy in the U.S. Office of Management and Budget.

** Martha K. Landesberg is the Associate Director for Privacy Policy and Education, Privacy Office, U.S. Department of Homeland Security. Previously, Ms. Landesberg has served as Director of Policy and Counsel for TRUSTe, as Of Counsel to the law firm of Dorsey & Whitney LLP, and as a Senior Attorney in the Federal Trade Commission's Division of Financial Practices.

[1] As this essay was being completed, the FTC released an updated staff report on self-regulatory principles for online behavioral advertising. *See* Press Release, Fed. Trade Comm'n, FTC Staff Revises Online Behavioral Advertising Principles (Feb. 12, 2009), *available at* http://www.ftc.gov/opa/2009/02/behavad.shtm (collecting FTC materials on behavioral advertising).

databases. A growing area of discussion is the extent to which Internet Protocol addresses—the basic information transmitted in each web session—should be considered "personally identifiable information" or "personal data" subject to data protection rules.

In significant ways, the debates about online advertising have become the vehicle for broader debates about how privacy will be protected in the future. The increasing detail available to online advertisers and search engines foreshadows similar issues for other technologies, such as locational information that is becoming feasible to track through Global Positioning Systems and cell phones. In the United States, the online advertising debates might be a preview for cross-sectoral privacy rules– online activities and advertising have both become so pervasive that governance of online advertising could merge into comprehensive governance of privacy.

One other major theme is how identification and authentication will be managed going forward. Under President Bush, the federal government pushed for new identity systems such as REAL ID (minimum standards for state driver's licenses) and E-Verify (electronic confirmation of eligibility for employment). At the same time, there were numerous policy initiatives to address identity theft, including state laws requiring notice of data breaches, and the new federal "Red Flags" rule. Identity and authentication will continue to raise difficult technical, policy, and political issues in the coming years, and one of the authors of this essay worked on a major study in 2008 that proposed how authentication programs should be assessed in the new administration.[2]

Part II of this essay describes the structure of Privacy Law Year in Review. Part III summarizes the articles in this issue written by scholars. Part IV then presents the key points from each of the thirteen student notes.

II. THE TASKS OF PRIVACY LAW YEAR IN REVIEW

The principle goal of Privacy Law Year in Review is to create a trustworthy, non-ideological, and clearly written annual review of developments in privacy law, with a focus on developments affecting the United States. It is one of three annual issues of *I/S: A Journal of Law and Policy for the Information Society*. Peter Swire is Faculty Editor for this issue and co-author of this essay. Peter Shane, also of

---

[2] PETER P. SWIRE & CASSANDRA Q. BUTTS, THE ID DIVIDE: ADDRESSING THE CHALLENGES OF IDENTIFICATION AND AUTHENTICATION IN AMERICAN SOCIETY (2008), http://www.americanprogress.org/issues/2008/06/pdf/id_divide.pdf.

the Moritz College of Law, is overall Faculty Editor of the Journal. Other current *I/S* issues include "Patent Reform" and a Celebration of the 10th Issue of *I/S*. Information about *I/S* is available at http://www.is-journal.org. For the second year, Martha Landesberg is co-author of this Introductory Essay and has co-supervised the student notes with Peter Swire. Martha Landesberg is Associate Director for Privacy Policy and Education in the Privacy Office of the U.S. Department of Homeland Security.

As was true in previous years, we are delighted this issue of Privacy Law Year in Review will be distributed to all members of the International Association of Privacy Professionals ("IAPP"). Under the leadership of Trevor Hughes, the IAPP has grown rapidly in recent years and now numbers over 5000 members. Privacy Law Year in Review is distributed in hard copy to all IAPP members and members can also sign up for passwords to get online access to all *I/S* issues.[3]

We at Moritz continue to work closely with the IAPP to provide high-quality content for privacy professionals, students, and scholars. In 2007, IAPP published *Information Privacy: Official Reference for the Certified Information Privacy Professional.* Peter Swire, Sol Bermann, and others from Moritz wrote the first edition, which is the official study material for the CIPP examination. The second edition is now in late stages of edits. This year, for the first time, many of the student authors took the CIPP examination in the course of working on their notes.

Privacy Law Year in Review focuses especially on developments from late 2007 through the early fall of 2008. Students began their research in 2007 under the leadership of *I/S* Editor-in-Chief Erin Wright and Privacy Issue Editors Megan Engle, Carla Scherr, and Stephen Wolfson. Student work after March 2007 was under the direction of *I/S* Editor-in-Chief Natalie Bennett and Privacy Issue Editors Nathaniel Arden, Nicki Elgie, and Gena Miller Shelton. This essay was completed in February 2009.

III. ARTICLES BY SCHOLARS IN THIS ISSUE

This issue features two articles by scholars that provide a compelling mix of empirical research and analytic results, focusing on the costs of reading privacy notices and research into data breach notices.

---

[3] For IAPP members who wish to activate their online access, contact Kimberly McNeill, IAPP Membership Services Coordinator (207.351.1500 x133/kim@privacyassociation.org).

Carnegie Mellon researchers Aleecia M. McDonald and Lorrie Faith Cranor document under-appreciated costs of privacy notices. Privacy protection in the United States has often been understood as a "notice and choice" model– a website gives notice of its privacy practices, and individuals then choose whether to provide their personal information. This notice-based approach has some key advantages, such as fostering efforts by organizations to define their privacy practices and ensuring that the FTC has jurisdiction to enforce against deceptive practices. Privacy notices might help develop a market in privacy, by allowing consumers to choose among providers based in part on the content of the privacy policy. In addition, basing privacy enforcement on an organization's privacy policy reduces the burden on regulators to promulgate rules that apply to diverse companies with diverse business models.

The new empirical work by McDonald and Cranor poses this question: "If website users were to read the privacy policy for each site they visit just once a year, what would their time be worth?" The answer is: a lot. This once-a-year read of privacy policies would have a U.S. opportunity cost of over $650 billion.

The McDonald and Cranor findings pose a new challenge to economists and others who believe that notice-based systems are the best available way to protect privacy. Compared to other regulatory approaches, notice-based systems appear less costly because they avoid the problems that occur when regulators write less-than-optimal rules about what data uses to permit. The McDonald and Cranor findings, however, emphasize the costs to consumers of reading privacy policies. These are economic costs to notice-based approaches that may offset some or all of the economic benefits.

The McDonald and Cranor findings may also be useful in broader regulatory debates about the role of notice. Notice-based approaches are a close intellectual fit with "neoclassical economics," which assumes that individuals are rational actors who maximize utility. The more recent movement called "behavioral economics" has focused on cognitive biases and other empirical measurements of ways that individuals process information and make decisions. In addition to the existing literature about behavioral economics, the McDonald and Cranor findings show another limit of notice-based approaches– the economic value of the time to make a decision may be worth more than making a good decision. In such circumstances, individuals will predictably make many sub-optimal decisions. Regulatory approaches that rely less on notice may thus be more desirable than hitherto appreciated.

Computer security experts Matt Curtin and Lee Ayres have contributed a two-part article about data breaches to this issue: *Using*

Science to Combat Data Loss: Analyzing Breaches by Type and Industry. The first part presents an improved taxonomy for types of data breaches, in the hopes that data will increasingly become available in forms that will assist security researchers in identifying what responses are appropriate. The second part describes statistically significant differences between sectors in the types of breaches that occur. This sort of diagnosis of types of breaches is potentially extremely useful– it can highlight what sorts of problems plague different sectors, leading to a more effective set of security responses.

The Curtin and Ayres statistics suggest that quite different problems exist in different sectors. The Health Care and Social Assistance sector reported a higher proportion of lost and stolen computing hardware, but reported an unusually low proportion of compromised hosts. This data suggests that outside hackers have not been a key problem in the health care sector, but that hard-disk encryption or other measures to reduce the harms from lost equipment may be a priority. Educational Services reported, by contrast, a high proportion of compromised hosts, but low rates of insider misconduct or lost equipment. These findings highlight the challenges for universities in how to maintain an open and experimental attitude in an era where outside hackers may disproportionately target university computers for launching system-wide attacks.

In the Public Administration sector, the proportion of compromised host reports was below average, but the proportion of processing errors was high. These findings may be consistent with a view that the government sector has sought to be fairly strict on security, but the sector struggles to have the resources and personnel sufficient to avoid processing mistakes. Finally, the Finance and Insurance sector showed the smallest proportion of processing errors, but the highest proportion of insider misconduct. It is comforting to learn that processing errors are low in this sector, because errors in financial accounts by definition are often expensive and harmful. At the same time, the findings reinforce the need for strict internal controls in this sector against insider attacks. Banks are where the money is, and modern bank theft can often be achieved most effectively by internal finagling of accounts.

The Curtin and Ayres article highlights the value of data breach statutes for research in the field of computer security. New statutes and regulations about data breach should likely be crafted in ways that will create usable data for researchers. Improved research, in turn, will enable different sectors to respond more effectively to the distinctive threats they face.

IV. AN OVERVIEW OF PRIVACY LAW IN 2008

The notes in this year's Privacy Year in Review are grouped into the following four categories: identity and data loss; online and locational privacy; medical and genetic privacy; and international issues.

A. IDENTITY AND DATA LOSS

Three notes examine issues of proof of identity and identity theft: (1) the federal E-Verify program, which employers increasingly use to check eligibility for employment; (2) new legal rules concerning identity theft, including data freeze legislation and the "Red Flags" rule; and (3) recent developments in data breach notice, where an important rationale for the notice is to reduce identity theft.

Lizzette Romero's note considers the privacy issues posed by E-Verify, the system administered by the U.S. Citizenship and Immigration Service ("USCIS") that enables employers to electronically determine newly-hired employees' eligibility for employment. Employers submit information in an employee's I-9 Form (including name, date of birth, Social Security number, and citizenship status) to E-Verify, which compares that information against the Social Security Administration database and Department of Homeland Security immigration databases and provides eligibility information in real time. The system returns a Tentative Non-Confirmation Notice ("TNC") for employees whose eligibility it cannot immediately verify. Employees who receive a TNC are able to contest it and seek correction of their records, and the law prohibits employers from firing or taking other adverse measures against employees based upon a TNC. Ms. Romero describes in detail how E-Verify is designed to function, and discusses current concerns about the program's efficacy, its vulnerability to misuse and abuse, and the efforts underway to strengthen it.

The use of E-Verify has climbed in the recent past, with one current estimate that about 100,000 employers use it out of seven million employers in the United States.[4] Participation is mandatory for all federal agencies. Federal government contractors and subcontractors were to be required to use the system as well, but the

---

[4] *See* Jaikumar Vijayan, *E-Verify Hiring Mandate Dropped from Stimulus Bill*, COMPUTERWORLD, Feb. 13, 2009, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127982&intsrc=hm_list.

Department of Defense and the General Services Administration recently delayed implementation of that requirement until May 2009, pending the Obama administration's regulatory review. Eight states currently require participation by at least some private-sector employers (some states require *all* to participate), and more states may follow their lead. As the note points out, the trend toward broader use of E-Verify has highlighted the need to address several key issues, not least of which are the burdens on both businesses and employees faced with having to navigate the TNC process. Critics of the system are concerned about the frequency with which eligible workers, such as foreign-born U.S. citizens, receive TNCs and may ultimately be denied employment, due to employer errors in entering data into E-Verify, incorrect or outdated information in the databases used by E-Verify, or other factors. While the precise extent of this problem is a matter of debate, both the critics and USCIS recognize the need to minimize these occurrences.

The note also discusses the potential for misuse of the E-Verify system, and even outright fraud, by employers. Some of E-Verify's critics are concerned that employers have fired, or taken other adverse actions against, employees who receive a TNC, or have failed to inform employees who receive a TNC about their right to have their records corrected. Others are skeptical of the system's ability to ensure that individuals who are in fact eligible for employment will not be discriminated against on the basis of national origin. The fraudulent use of Social Security numbers and alien numbers by employers (and by some employees) participating in E-Verify is another ominous development. Ms. Romero's note concludes with a discussion of recent efforts to address these issues. Political debates about E-Verify are likely to continue. For instance, the House version of the stimulus bill at the beginning of the Obama administration would have required participation in E-Verify by recipients of federal funding, but the final version of the bill omitted that requirement.

Nicki Elgie's note addresses identity theft, which remains a significant problem in the United States despite the Herculean efforts of state legislators, state and federal agencies, the President's Identity Theft Task Force, and consumer and business groups. The note begins with a description of state laws that provide consumers the right to have a "security freeze" placed upon their credit reports. Such freezes are one way to thwart identity thieves who seek to obtain credit reports under false pretenses or to open revolving credit accounts (or to incur other debt) using stolen information. The note briefly discusses bills pending in the Congress that would establish a federal credit freeze regime.

The note also analyzes the "Red Flags" rule promulgated jointly by the FTC and the federal bank regulatory agencies, as required by the Fair and Accurate Credit Transactions Act of 2003. The rule requires financial institutions and creditors to identify specific practices, behaviors, or patterns of activities that are indicative of identity theft—"red flags"—and to implement policies and procedures to detect and address them. As the note points out, the rule follows the example of the Gramm-Leach-Bliley Safeguards rule by allowing businesses flexibility in designing their required programs. The note concludes with an analysis of the likely efficacy of both the state freeze laws and the Red Flags Rule in protecting consumers from identity theft. Although the rule initially required companies to come into compliance by November 1, 2008, the FTC has announced that it will delay enforcement of the rule as to companies under its jurisdiction until May 1, 2009.

Julie Heitzenrater's note provides an overview of recent state and federal developments in breach notice legislation. It describes the similarities and differences among various enactments and proposed legislation in the states, including the types of personal information protected, the conditions necessary to trigger notice to consumers, standards for reporting breaches to the government, and the role of encryption. The note also analyzes proposed state legislation that would hold retailers liable to financial institutions and credit card issuers for damages (e.g., the costs of canceling and reissuing credit or debit cards, or refunds of unauthorized charges) resulting from a breach of the retailers' databases. Some of these bills would impose strict liability for a data breach; others would provide for liability where a retailer has retained the card access security code, PIN verification code, or magnetic stripe data after a transaction has been approved, in violation of standards required of retailers by credit and debit card issuers. The note summarizes the arguments in support of and in opposition to these bills. The note also discusses federal legislative efforts to date to move breach notification legislation, and the market forces which, together with state legislation in this area, are working as incentives to businesses to bolster the security of their databases even in the absence of federal legislation.

B. ONLINE AND LOCATIONAL PRIVACY

Four notes this year address issues of online and locational privacy: the scope of the term "personally identifiable information," and especially whether an Internet Protocol ("IP") address should be subject to privacy protections; the ongoing debate about privacy and

behavioral profiling; special rules that apply to children online, including for social networking sites such as MySpace and Facebook; and privacy issues that arise as global positioning systems become more pervasive, so that the locations of individuals at least potentially can become more widely tracked by public and private entities.

Frederick Lah's note reports on the current debate over whether IP addresses should be considered "personally identifiable information," or "personal data" in European parlance, and thus subject to regulation under U.S. law and the E.U. Data Protection Directive. The note begins with a discussion of the shift that is occurring from mostly dynamic IP addresses, which are relatively difficult for a website to link to an individual, to static IP addresses, where the persistence of the IP address over time increases the likelihood that a website will have the opportunity to identify an individual. Broadband services often provide a static IP address for each user, and the coming shift to the new protocol called "IPv6" will increase the portion of users with static IP addresses. These technological and market shifts strengthen the argument that IP addresses can now be tied to individuals and thus constitute "personally identifiable information" or "personal data."

The note examines the recent history of this topic in the European Union. The E.U. Article 29 Working Party has, on several occasions, expressed its view that IP addresses are "data related to an identifiable person," and that Internet service providers must therefore treat them as "personal data" subject to the protections of the E.U. Data Protection Directive. In its April 2008 *Opinion on Data Protection Issues Related to Search Engines*, the Working Party concluded that search engines must also treat dynamic and static IP addresses as "personal data" unless there is "absolute certainty" that individuals with whom IP addresses are associated cannot be identified. The European Union has yet to take official action on the *Opinion*, but it is bringing pressure to bear on the search engines to shorten the period of time for which they retain data (including IP addresses). The note also examines the history of the issue in the United States, highlighting the relevant definitions under various statutes and in connection with behavioral advertising. The note concludes with a summary of arguments both for and against extending privacy protections to IP addresses.

James Schedwin's note discusses the ongoing debate about privacy and behavioral advertising. This note defines important terms used in online advertising, such as "contextual" advertising (different ads are served based on where a user is on a website) and "behavioral" advertising (different ads are served based on the historical activities of a user or a user's device). The note examines the significant recent

mergers among online advertising firms, which led most visibly to a split FTC decision in late 2007 approving the merger of Google and DoubleClick. The day the merger was approved, the FTC proposed self-regulatory guidelines for online behavioral advertising. The note analyzes the extensive public comments on these guidelines, highlighting key issues going forward such as notice, choice, and the use of sensitive data.

Another ongoing controversy has revolved around the measures that should be implemented to protect the safety of children online. The explosive growth of online social networking has led to concerns about the safety of children who are drawn to "general audience" sites such as MySpace and Facebook. Potential threats to young children in these online environments range from the disclosure of sensitive personal information (by children themselves, but also by others) to cyber-bullying, exposure to pornography and other content unsuitable for children, and child predation. Lawmakers, regulators, technology experts, children's advocates, and the social networking sites themselves have invested a great deal of time and effort to identify and implement strategies to address these threats. Matthew Whitman's note explores the issues posed by one such strategy: the use of age verification as a means of limiting children's access to social networking sites.

The note first discusses the January 2008 agreement between MySpace and forty-nine state attorneys general—following a lengthy investigation by some of these officials into sexual predators' activities on the site—in which MySpace committed to a set of "Key Principles" for protecting children from online predators and other threats in the social networking space. Among other things, MySpace agreed to create a registry of e-mail addresses provided by parents who want to restrict their children's access to the site and to establish a task force to develop automated age and identity authentication tools for use on social networking sites in general. The agreement serves as the springboard for the note's discussion of the technical and policy arguments concerning the efficacy of age verification as a means of enhancing children's safety online.

As the note points out, critics of age and identity verification see centralized registries as tempting targets for hackers and identify thieves. They believe that automated verification tools will be easily circumvented by those who do not wish to be identified, including internet-savvy children. Proponents of age verification are more optimistic about the role technology can play in addressing these issues. For example, the FTC has suggested that age verification technology could serve as a substitute for the age-screening techniques it had previously recommended (e.g., using a session

cookie to prevent children from re-entering a site after having been denied access because of their age).[5] The Commission expressed the hope that growing concerns about children's safety on social networking sites would ultimately jump-start a market for age verification technologies.

The note discusses alternatives to age verification for addressing children's safety on social networking sites, including the use of filtering software, resources such as Getnetwise.org and other websites devoted to teaching online safety, and the role of parents in monitoring their children's online activities. The note concludes by highlighting the work that social networking sites are doing to prevent young children from creating online profiles and to explore other approaches, including age verification.

Sarah Rahter's note examines another realm where technology is enabling tracking at a level of detail that historically was not possible. With the spread of Global Positioning Systems ("GPS") in automobiles and the pervasive use of cell phones, the location of individuals is becoming knowable in ways that were technically impossible a decade ago. Ms. Rahter focuses on the legal rules and policy for government access to this treasure-trove of locational data. The note shows the relatively weak protections under the Fourth Amendment for both GPS and cell phone locational data, and examines key states, which have varying levels of protection under their constitutions and statutes. One area where courts have recently split is the legal standard that the federal government must meet to gain access to cell phone location records in real time. The note concludes with a discussion of a new book by law professor Christopher Slobogin about how the Fourth Amendment should be interpreted for these sorts of high-technology searches.

C. MEDICAL AND GENETIC PRIVACY

Four notes this year explore issues of medical and genetic privacy. Topics include: the Genetic Information Nondiscrimination Act of 2008, which creates new federal non-discrimination requirements in employment and health insurance; the rules applying to genetic information used in scientific research; the legal status and policy debate about keeping tissue samples for DNA testing; and issues of

---

5 FED. TRADE COMM'N, IMPLEMENTING THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT: A REPORT TO CONGRESS (2007), http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf.

familial privacy for parents who oppose mandatory vaccination for their children.

Jennifer Lee's note explains the history and implications of major legislation enacted in 2008, the Genetic Information Nondiscrimination Act ("GINA"). The Human Genome Project of the 1990s vastly increased the amount of genetic knowledge available to researchers, and potentially to employers and insurers. Most states passed at least some nondiscrimination laws in this area, but the laws varied greatly and some had large loopholes. After nearly a decade of debate, Congress passed GINA in May 2008. As the note explains, GINA forbids employers and health insurers from discriminating on the basis of genetic information. Major implementing rules are scheduled to be announced in 2009, and debates may continue about whether and how to extend GINA's protections to life insurers and others.

Sarah Fendrick's note discusses federal and state privacy protections for individuals whose genetic information is used in scientific research. These research uses are generally outside the scope of GINA. The note begins with an analysis of gaps in current federal protections. The HIPAA Privacy Rule applies only to "covered entities" such as medical providers. Researchers who use genetic information, however, are often outside of the scope of HIPAA. A legal gap also exists under the federal Common Rule, which requires the informed consent of research subjects and approval by an institutional review board for research within its scope. The Common Rule, however, applies only to research funded or conducted by a federal agency, and only to research that uses human subjects. Thus, neither HIPAA nor the Common Rule applies to many types of privately-funded genetic research (including research by many, if not most, new biotech companies). State-funded research, or research on genetic material but not human subjects, also falls outside of the federal protections.

As Ms. Fendrick notes, twenty-nine states have taken steps to address the gaps in federal coverage, but the state laws expressly regulating the use of genetic information for genetic testing and other purposes vary widely in the types of information they govern and in the extent of the protections they require. Ms. Fendrick discusses the pros and cons of various means short of legislation for addressing the privacy of genetic information held in research databases, from de-identification and other forms of data masking to using only research subjects who consent to public disclosure of their data. The note concludes by urging Congress to amend HIPAA by expressly defining genetic material as Personal Health Information and to regulate

entities that are not currently subject to the HIPAA Rule or the Common Rule.

Natalie Bennett's note concerns the privacy implications for the current trend toward expanding state and federal databases of tissue samples taken from criminal offenders for DNA testing. As scientific understanding of DNA has progressed, so has appreciation for the complexity of the personal information that can be derived from DNA. As Ms. Bennett points out, DNA samples, unlike fingerprints, can do more than simply place an individual at a crime scene– they also provide insights into that individual's genetic history, kinship history, and predisposition to certain medical conditions. The note examines state and federal law governing DNA databases and federal court decisions in cases challenging the collection and storage of genetic information on Fourth Amendment grounds. The constitutional challenges to such collection and storage have not succeeded to date. The note also considers the arguments for and against creating a national database of DNA samples from all individuals, and the role that national standards could play in protecting information in DNA databases from unauthorized access and misuse.

Ms. Bennett explores important issues underlying the debate about the appropriate role of DNA databases. The states are the primary sources of tissue samples that generate DNA profiles, and state DNA databases are linked through a national indexing system. Almost all states either require or permit the indefinite retention of tissue samples, raising concerns about the vulnerability of information in DNA databases to unauthorized access and misuse. Although both state and federal law place certain limitations on access to and disclosure of information in DNA databases, there is no uniform standard for access or disclosure, or for retention of DNA samples. The potential for "mission creep" is a closely related concern. Critics of the expanded use of DNA databases argue that, in the absence of mandatory privacy protections for sensitive DNA data, it is increasingly likely that government and private-sector entities will obtain access to this information for purposes unrelated to law enforcement. Ms. Bennett presents the arguments for implementing national legal standards for DNA databases, based on fair information practice principles, including purpose specification and use limitation.

Kyla Kelch's note focuses on the legal and social arguments associated with the growing phenomenon of parental opposition to state laws mandating the vaccination of children against communicable diseases. The note recounts the public health rationale for vaccine mandates, and analyzes their implications for privacy. It considers the various statutory exceptions that parents rely upon to avoid immunizing their children (e.g., for religious, philosophical,

and/or health reasons) as extensions of parental privacy rights. The note also focuses on the current status of state immunization information systems, or immunization registries, which serve as repositories for children's personally identifiable information, including vaccination histories, submitted by health care providers. The note describes the privacy concerns raised by such systems, including concerns about confidentiality and the potential that the information will be used for purposes other than tracking vaccinations. The note concludes with an analysis of a current proposal for a national framework to strengthen the privacy protections for state immunization registries.

D. INTERNATIONAL ISSUES

This year's two international notes focus on Japan and China. Ryan Waggoner is combining his law studies with a master's degree in Japanese law. His note compares privacy protections in the U.S. and Japanese financial services sectors. He uses his Japanese language skills to analyze key documents that have not been previously brought to an English-language audience. Mr. Waggoner explains that the Japanese approach lies between the U.S. sectoral and the E.U. omnibus approach to privacy regulation. Japan enacted the economy-wide Act for the Protection of Personal Information in 2003, but actual implementation depends a great deal on sector-by-sector guidelines issued by government ministries, including for the financial sector. For the financial sector, the definition of "personal information" applies essentially to any commercial actor that uses financial personal information; this data-centered approach contrasts with the U.S. approach, where some companies are "financial institutions" covered by Gramm-Leach-Bliley, but where other companies fall outside of the law's protection. Mr. Waggoner also explains that the legal requirements concerning notice and opt-out are stricter in Japan than under Gramm-Leach-Bliley.

Aimee Yang's note explains two major developments in China. The first is that China appears to be on the path to creating a national data protection regime. A first version of a draft law was completed in 2005, but that version was not implemented. Substantial discussions about a national law have continued since that time, with twin goals: enable China to trade more easily with European and other countries that have strict data protection regimes and avoid undue burden on economic growth. Ms. Yang's note explains recent developments in the debates in China, and highlights key issues, including how to take account of differing cultural attitudes toward "privacy."

Ms. Yang's note also analyzes the ongoing international trade dispute about whether China will develop encryption standards that differ from global standards. Non-Chinese companies and governments have expressed serious concerns about such Chinese-specific standards. Any mandate within China to use Chinese-specific encryption has been criticized as a protectionist measure in violation of World Trade Organization rules. Use of China-specific standards may also compromise data security– the Chinese standards have not been approved as secure by international standards bodies. Global information security may thus be weakened if Chinese-manufactured components, included in many devices, are based on insecure encryption. Although China has recently withdrawn the proposed mandates, this issue may recur in the future.

V. CONCLUSION

At the time of this writing in February 2009, the new Obama administration has said little about privacy. The initial economic stimulus package included substantial amendments to the HIPAA medical privacy rule, including new data breach notice requirements, extension of the statute to business associates, and stricter rules in areas such as marketing and accounting of disclosures to patients. Most of the provisions, however, are derived from bills that were considered in the House of Representatives in 2008. There are thus few clues yet available about how the new administration will address privacy issues.[6]

Looking forward, one over-arching question will be the extent to which the United States will continue to rely on self-regulation to the same extent as it has previously. Those who oppose government regulation will point to the severe economic slump, and argue that Congress and the new administration should be reluctant to put additional burdens on business during hard economic times. On the other hand, many observers have criticized self-regulation on Wall Street, and have argued that the lack of mandatory federal rules contributed to the financial collapse. President Obama was elected with the promise of change, but the shape of such change in the privacy realm remains difficult to predict.

---

[6] The most detailed Obama campaign statement about privacy is contained in *Barack Obama: Connecting and Empowering All Americans through Technology and Innovation*, which is available at http://www.barackobama.com/pdf/issues/technology/Fact_Sheet_Innovation_and_Technology.pdf (last visited March 29, 2009).